An Act Concerning Electricity and Energy Efficiency
Public Act 07-242
Section 8

White Paper on the Security of Siting Energy Facilities

Prepared by the Connecticut Siting Council
October 8, 2009

INTRODUCTION

In response to Public Act 07-242, "An Act Concerning Electricity and Energy Efficiency", the Connecticut Siting Council (Council) issues this white paper to establish the Council's scope of review of energy security in regards to the siting of electric transmission and generating facilities. This policy document was developed to comport with relevant parts of Section 8 of the Public Act which states:

> Not later than September 1, 2007, the Connecticut Siting Council, in consultation with the Emergency Management and Homeland Security Coordinating Council, established pursuant to sections 28-1b of the general statutes, and the Department of Public Utility Control shall initiate a contested case proceeding, in accordance with the provisions of chapter 54 of the general statutes, to investigate energy security with regard to the siting of electric generating facilities and transmission facilities, including consideration of planning, preparedness, response and recovery capabilities. The Connecticut Siting Council may conduct such proceedings in an executive session with sensitive information submitted under a protective order.

Pursuant to legislative intent of the Act, this document will review existing regulations and guidelines regarding security for the siting of electric generating and transmission facilities. Energy security is a broad area of review, one that, ironically, grows ever more complex as the nation's energy system becomes more integrated. Security remains a broad concept even when limited to the Council's task of siting—that is, determining the particular locations in Connecticut where electric generating or transmission structures should be placed. The Council will focus mainly on physical threats, as opposed to cyber threats, to electric generating and transmission facilities and on threats that are intentional, ranging from simple trespassing to vandalism to dedicated acts of sabotage.

Generally speaking, siting security in this document does not relate to operational, reliability, and maintenance procedures affecting electric facilities, asset connection requirements, or naturally-caused calamities (for example, hurricanes or ice storms). Most of these security concerns are predictable and the Council already factors them into its siting decisions. Moreover, most storm threats involve the electric distribution system, which is not under the Council's purview.

EXISTING STANDARDS/GUIDELINES

The protection of electric generating and transmission facilities is one of the highest priorities for national/international, regional, and state authorities and organizations, and involves many existing layers of regulation and guidelines issued and monitored by various entities, both public and private. Also, this elaborate security protection regime has built-in mechanisms for updating and changing. Below is a brief overview of the primary existing organizations and procedures that ensure protection for the grid.

National
Presidential Decision Directive 63 "Protecting America's Critical Infrastructures", issued in May 1998, identifies "electricity" as a critical infrastructure. This directive required the U.S. Department of Energy (DOE) to be the lead agency for the protection of critical energy infrastructure (Electricity Sector). The DOE, in turn, designated the North American Electric Reliability Corporation (NERC) as the Electricity Sector Coordinator.

NERC's responsibilities as Sector Coordinator include the following:

- assessment of sector vulnerabilities;
- planning to reduce electric system vulnerabilities;
- development of a system for identifying and averting attacks;
- development of a notification procedure for sector participants and appropriate government agencies when an attack is imminent or underway; and
- assistance in reconstituting minimum essential electric system capabilities after an attack.

In June 2002, NERC issued "Security Guidelines for the Electricity Sector", Version 1.0, that describe general approaches, considerations, practices, and planning philosophies to be applied in protecting electric system infrastructure. The guidelines are voluntary in nature and were developed to help entities develop policies, procedures, practices and strategies to address issues related to security. Each entity can decide if the particular guideline will be used and to what extent, if any. These guidelines, with subsequent additions and revisions, include the following topics:

- Communications
- Continuity of Business Practices
- Continuity of Operations
- Control System - Business Network Electronic Connectivity
- Control System Cyber Security Incident Response Planning
- Patch Management for Control Systems
- Securing Remote Access to Electronic Control and Protection Systems
- Cyber - Access Controls
- Cyber - Intrusion Detection
- Cyber - IT Firewalls
- Cyber - Risk Management
- Employment Background Screening
- Vulnerability and Risk Assessment
- Protecting Potentially Sensitive Information
- Emergency Plans
- Physical Response
- Physical Security

- Physical Security - Substations

In addition to the aforementioned guidelines document, separate voluntary guideline documents were established, as follows:

- Security Guideline for the Electricity Sector -- Threats and Incident Reporting - Version 2, April 2008;
- Security Guideline for the Electricity Sector -- Physical Response - Version 3.0, November 2005; and
- Threat Alert System and Cyber Response Guidelines for the Electricity Sector -- Version 2.0, October 2003.

Although these guidelines remain voluntary, the Energy Policy Act of 2005 delineated a process leading to the development of mandatory standards. The 2005 act authorized the Federal Energy Regulatory Commission (FERC) to designate a national Electric Reliability Organization (ERO). In July 2006, FERC issued an order that certified NERC as the ERO for the United States. Subsequently, NERC transformed many existing voluntary policies into mandatory standards to ensure the proper design, operation and maintenance of the electric system.[1] Standards were developed to address aspects of the design, operation, and maintenance of electric infrastructure, including security.

Security is addressed in the daily operation of the electricity grid and in future planning for the grid. NERC operates the industry's Electricity Sector Information Sharing and Analysis Center (ESISAC) under the U.S. Department of Homeland Security and Public Safety Canada. ESISAC gathers information about security-related threats and incidents, and communicates it to government authorities.

NERC is continually evaluating and modifying its security standards and guidelines to address changing technologies and emerging threats through the Critical Infrastructure Protection Committee (CIPC). Comprised of industry experts in the areas of cyber security, physical security, and operational security, the CIPC coordinates all NERC's security initiatives.

In addition to NERC, the IEEE (formerly known as the Institute of Electrical and Electronics Engineers, Inc.), a professional organization dedicated to the advancement of technology, has taken the initiative on security. Its security guideline, Standard 1402-2000 – IEEE Guide for Electric Power Substation Physical and Electronic Security, issued in June 2000, addresses security issues related to human intrusion during the construction, operation, and maintenance of electric power supply substations. Methods to deter and mitigate intrusions are discussed.

Regional and Interregional

The Northeast Power Coordinating Council (NPCC) is the regional organization that is responsible, under NERC, for the reliability of the electric system throughout Northeastern North America (New York State, the six New England states, and, in Canada, Ontario, Quebec, and the Maritime provinces). NPCC has reliability criteria that address all aspects of the grid, including security. The NPCC criteria have been written to be consistent with the NERC reliability standards, but in some cases they are more stringent and more specific.[2]

[1] Link to NERC standards web page: <http://www.nerc.com/page.php?cid=2|20>

[2] Link to NPCC documents web page: <http://www.npcc.org/documents/regStandards/Criteria.aspx>

Under NPCC, the Independent System Operator for New England (ISO-NE) is the Regional Transmission Organization (RTO) responsible for ensuring the reliability of the electric system in New England. ISO-NE generally carries out the NPCC reliability criteria—security criteria among them—but also has some of its own security procedures.[3]

Furthermore, as an independent ISO/RTO among its North American peers, ISO-NE participates in various kinds of interregional planning activities and other exercises designed to smooth the transitions between electric systems in different parts of the U.S. and adjoining North American territory, activities that frequently involve sharing ideas and coordinating around security issues. For instance, ISO-NE is part of a Joint ISO/RTO Planning Committee that specifically addresses cross-border aspects of transmission security.

State

At the state level, attending to energy security in its broadest sense, namely, long-term energy sustainability and reliability, is the job of policy and planning bodies such as the Connecticut Energy Advisory Board, the Office of Policy and Management, the Energy Conservation Management Board, and several others. On more immediate aspects of electric system security, the Department of Emergency Management and Homeland Security (DEMHS) coordinates with the utility companies. The Council typically considers physical security of electric facilities during the application process, as necessary.

COMPLIANCE

All bulk power system owners, operators, energy marketers, generators with contracts to sell energy, and local distribution companies must comply with NERC-approved operational and reliability standards. In Connecticut, these entities are required to register with NERC through the Northeast Power Coordinating Council (NPCC), the regional organization that ensures reliability to Northeastern North America. Both NERC and the NPCC conduct compliance reviews to enforce the required standards through assessments, audits, evaluations, investigations and analysis of self-reporting requirements. Entities that do not meet certain criteria are subject to enforcement action through fines or other sanctions.

COUNCIL'S ROLE

Although the task of developing security for the siting of certain aspects and components of electrical infrastructure has been and continues to be examined and addressed by national/international, regional, and state authorities and organizations, the Council will consider specific discussion points in regards to security. The Council's expertise in assessing siting criteria for electric facilities will facilitate heightened awareness and provide for a unique insight regarding security concerns. In addition to these discussion points, the Council will solicit comment from the DEHMS regarding siting security concerns.

The Council may examine these discussion points to ensure that security procedures and standards are consistent with existing guidelines, standards and other criteria. The discussion points probed by the Council may vary from application to application, depending on various factors, and in some cases the number of security questions may be minimal.

[3] Link to ISO-NE procedures: <http://www.iso-ne.com/rules_proceds/index.html>

Some questions asked in the prospective reviews may elicit answers that are highly sensitive. Applicants seeking to submit proprietary information under protective orders shall follow the Council's established procedures.

In considering applications for a Certificate of Environmental Compatibility and Public Need or a Petition for a declaratory ruling, and consistent with PA 07-242 Section 8, the Council will examine security issues around four discussion areas, including but not limited to: Planning, Preparedness, Response and Recovery. The general area of discussion for each topic is presented below.

A. PLANNING

1. **Identification**
   Identify the physical vulnerabilities most likely to pose a security threat.

2. **Facility type/characteristics**
   Identify the type and characteristics of the facility and any ways in which the facility's setting affects security concerns.

3. **Interdependencies**
   Examine any pertinent ways in which the facility is linked to other facilities and systems and potential repercussions from a facility or system interruption.
   Examine whether the proximity of the facility to other electric facilities, either dependent or independent, presents security challenges.

4. **Awareness**
   Examine if there is an established method to help regional, state and national security officials maintain situational awareness of this facility.

B. PREPAREDNESS

1. **Support infrastructure**
   Examine site security infrastructure, including site monitoring, physical and non-physical barriers and access controls.

2. **Personnel**
   Review any simulated exercises that include local police, fire, and other emergency response teams.
   Examine whether local law enforcement/emergency response liaison is in place, and review mutual aid agreements between affected entities.

C. RESPONSE

1. **Access to information**
   Examine notification procedures to public and/or local officials, including the types of security issues that would warrant such notification.

2. **Mitigation**
   Examine mitigation measures, including alternate routing of power, strategically located spares and mobile backup generation.
   Examine whether procedures are in place to ensure that mitigation protects natural resources at the site.

D. RECOVERY

1. **Recovery Measures**
   Identify measures that will be taken, if necessary, to restore natural resources at the site of the facility.

2. **Reporting**
   Determine whether reporting procedures are established to evaluate and improve the effectiveness of local emergency response teams, methods to limit negative impacts on neighboring electric facilities, and restoration of the natural environment.

CONCLUSION

The Council recognizes and agrees that electricity is a critical infrastructure as defined by Presidential Decision Directive 63, "Protecting America's Critical Infrastructure". The Council may also add its own prospective site security review. In doing so, the Council notes that while redundancy is sometimes a problem in any regulatory review, strategic redundancies are actually safeguards. The Council believes that its long-established focus on the local particulars of proposed electric facilities can contribute to the physical security of the grid.